

Auditing Information Security

Lindsay M. Harris, CISA
California State Auditor's Office
September 13, 2016

CALIFORNIA STATE AUDITOR



Clarifying Issues •
Formulating Solutions •
Positively Impacting Californians •

◆ Introduction/Agenda

- Our Approach
- What We Found
- The Cause
- What We Recommended
- The Outcome



Our Approach

- Identified Certain Requirements to Test
 - Information Asset Management
 - Risk Management
 - Information Security Program Management
 - Information Security Incident Management
 - Technology Recovery

Our Approach

FOUNDATION
of Information Security Control Structure



Information Asset Management

Reporting entities should establish and maintain an inventory of their information assets and determine the necessary level of security for each.



Risk Management

Reporting entities should identify and consistently evaluate potential risks to their information assets.



Information Security Program Management

Reporting entities should develop and continually update programs for protecting their information assets from the risks they have identified.

Information Security Incident Management

Reporting entities should develop and document procedures to ensure their ability to promptly respond to, report on, and recover from information security incidents such as malicious cyber attacks.

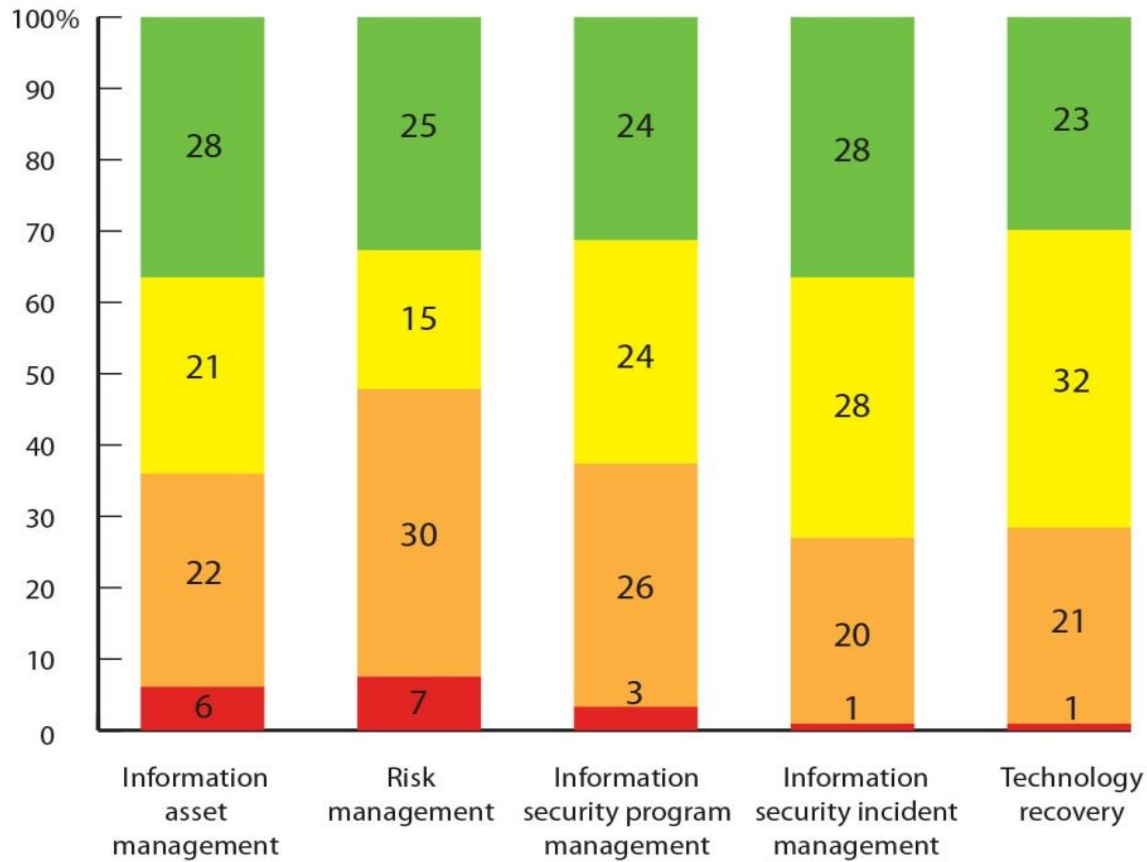
Technology Recovery

Reporting entities should create detailed plans to recover critical information assets from unanticipated interruptions or disasters such as floods, earthquakes, or fires.

Our Approach

- Reviewed Department Compliance Reports
 - Self-Reported Compliance Status
- Surveyed Over 100 State Entities
 - 77 Entities Responded

Survey Says



◆ What Is Really Going On?

- Selected Five Reporting Entities to Conduct On-site General Control Review
 - Collect, Store or Maintain Sensitive Data
 - Self-Reported Compliance in 2014
 - Diverse Sizes and Responsibilities

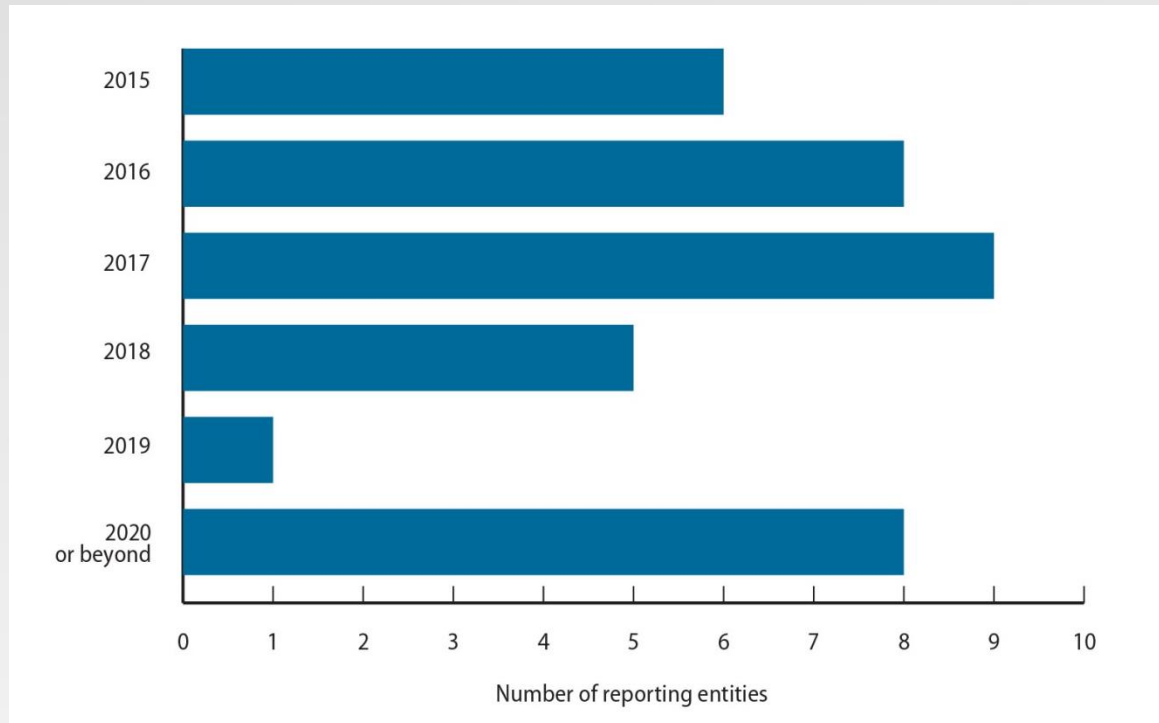
What is Really Going On?

REPORTING ENTITY	ENTITY DESCRIPTION	COLLECTS, STORES, OR MAINTAINS			INFORMATION ASSET MANAGEMENT	RISK MANAGEMENT	INFORMATION SECURITY PROGRAM MANAGEMENT	INFORMATION SECURITY INCIDENT MANAGEMENT	TECHNOLOGY RECOVERY
		PERSONAL INFORMATION OR HEALTH INFORMATION PROTECTED BY LAW	CONFIDENTIAL FINANCIAL DATA	OTHER SENSITIVE DATA					
A	Provides critical state services	Yes	Yes	Yes	Orange	Orange	Orange	Orange	Orange
B	Administers federal and state programs	Yes	No	No	Orange	Green	Green	Yellow	Yellow
C	Oversees an entitlement program	Yes	Yes	Yes	Orange	Orange	Orange	Orange	Orange
D	Performs enforcement activities	Yes	No	Yes	Red	Orange	Red	Red	Orange
E	Manages critical state resources	Yes	No	Yes	Orange	Red	Orange	Yellow	Yellow

Why?

- Lack of Effective Oversight
 - The Department of Technology Was Unaware
 - 37 of 41 Survey Respondents Had Certified Compliance to the Department
 - Some Entities' Weaknesses Persisted For Years
 - The Department of Technology Did Not Always Follow-up on Remediation Plans
- Lack of Guidance and Training

When Do Entities Expect to Comply?



What We Recommended

- Mandate Biennial Security Assessments
- Authorize the Department of Technology To Redirect Funds to Remediate Weaknesses
- Improve IT Oversight Practices at the Department of Technology

◆ What Has Happened?

- Governor's Executive Order: California Cybersecurity Integration Center
 - To strengthen California's cybersecurity strategy and improve inter-agency, cross-sector coordination
 - Central hub for state government's cybersecurity
 - Coordinate information sharing
 - Broadly represented
 - Cyber Incident Response Team

◆ What Has Happened?

- Enacted AB 670
 - At Least 35 Security Assessments Annually
 - Establish Assessment Requirements
 - Entity Being Assessed Funds the Assessment
 - Share Results with California Office of Information Security and Office of Emergency Services

◆ What Has Happened?

- The Department of Technology Made Changes
 - Adopted Nationwide Cyber Security Review Self-Assessment
 - Established a Plan of Action and Milestone Tool
 - Expanded Ongoing Risk-Based Audit Program
 - Partially Implemented Other Recommendations

What Has Happened?

- Continual Legislative Interest
 - Legislation Passed
 - Legislative Oversight Hearings
 - Considering Future Audit Work

◆ More Information?

- Report #2015-611, Details The Results of This High Risk Audit
- Report #2014-602, Designated Oversight of IT Projects a High Risk Issue
- Report #2013-601, Designated Oversight of IT Controls a High Risk Issue

» www.auditor.ca.gov